SEGURIDAD FÍSICA, PREVENCIÓN Y DETECCIÓN

María de Jesús Antonia Ochoa Oliva
UANL-FCFM
Universidad Autónoma de Nuevo León
Facultad de Ciencias Físico Matemáticas
San Nicolás de los Garza, Nuevo León, México

Resumen:

Este trabajo explica las variables que juega la seguridad física en las organizaciones, ya que es un conjunto integrado de capacidades y soluciones que deben proveerse en una organización o centro de cómputo para mantener la seguridad informática en un nivel aceptable. Uno de los errores más comunes es que estas se centren en el hardware y no en el soporte de las aplicaciones; por ello es importante saber dónde se alojará la infraestructura tecnológica que ayudará a la continuidad de la operación. Además, se hace referencia a las barreras físicas y mecanismos de control en el entorno de un sistema informático para proteger el hardware de amenazas físicas complementada con la seguridad lógica.

Palabras claves:

seguridad física, amenazas, continuidad de negocio, seguridad informática

Introducción

Las principales amenazas de un sistema informático son los desastres naturales, incendios accidentales, tormentas, temperaturas extremas, terremotos e inundaciones que conllevan consecuencias catastróficas; asimismo, se presentan amenazas ocasionadas por el hombre como pueden ser disturbios, sabotajes internos o externos en forma deliberada, etc. La seguridad física previene cada una de las anteriores.

¿Qué es la seguridad física? Es la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". [1]

El buen estudio de la infraestructura tecnológica que se va a instalar en un edificio y el análisis del entorno físico son partes fundamentales para que se soporten las aplicaciones o sistemas de hardware o software; todo este estudio es para llevar a cabo la minimización de riesgos y generar una continuidad de operación en las organizaciones.

Revisando las principales amenazas, vulnerabilidades, ataques, se establece un esquema de prevención, donde se establece una detección y así mismo se realizan las medidas establecidas por las políticas de seguridad.

Las medidas de detección que se recomiendan son:

- Mantener las máquinas actualizadas y seguras físicamente
- Mantener personal especializado en cuestiones de seguridad
- Los administradores de red deben configurar en forma adecuada.
- Mantenerse informado constantemente sobre cada unas de las vulnerabilidades
- Control de acceso, la restricción de los derechos de acceso a las redes, sistemas, aplicaciones, funciones, edificios y datos
- Seguridad de la información de manejo de incidentes, anticipar y responder adecuadamente a las violaciones de la seguridad de información
- Gestión de la continuidad, proteger, mantener y recuperar los procesos críticos de negocio y sistemas
- Cumplimiento, garantizar la conformidad con las políticas de seguridad de la información, normas, leyes y reglamentos [2]

Cuando se habla de un estudio del entorno físico, significa que se debe de realizar un levantamiento de datos que lleve a tomar decisiones que den cómo resultado la ubicación del hardware, dispositivos de red, centros de cómputo, etc., en este estudio se revisa la ubicación del edificio, acceso físico de personas, la interconexión de cableado de datos y eléctrico, controles de temperatura interna y externa, condiciones climáticas, tipo de montaje de hardware y software, métodos de administración de acceso a los sistemas de hardware, revisión de la continuidad y operación de cualquier sistema.

La seguridad física en forma específica se torna ardua, puesto que la operación misma se lleva a cabo por parte de los usuarios y se generan vulnerabilidades, ya sea intencionadas o imprudenciales, de tal manera que para los gestores de la seguridad informática es importante hacer cumplir las políticas de seguridad como la parte normativa.

Las medidas específicas de seguridad física incluidas en las normas o políticas se desarrollan con base en las condiciones en que se requiere proteger las instalaciones y siempre tener en cuenta los siguientes factores: grado de clasificación de la información, tipo de información en cuanto a su origen, cantidad y formato de información ya sea en papel o electrónico, necesidad de conocer el personal, amenazas y vulnerabilidades, medios de almacenamiento de información, todas estas medidas de seguridad serán aplicables cuando:

- Impedir la entrada por parte de intrusos, tanto si se emplean métodos subrepticios como si utilizan otros que impliquen el uso de la fuerza
- Disuadir, impedir o detectar acciones llevadas a cabo por personal desleal
- Permitir la limitación del personal en su acceso a información clasificada de acuerdo con el principio de la necesidad de conocer
- Detectar posibles brechas o violaciones de seguridad y ejercer las pertinentes acciones de corrección sobre estas con la mayor brevedad posible. [3]

Prevención

En el momento que se requiera ser preventivos se debe de empezar con los diferentes roles de los recursos humanos, realizando una estructura organizacional con grados de responsabilidad y desarrollo de la custodia de la información; no se debe de olvidar que la buena clasificación de procesos y recursos nos lleva a generar

protocolos de seguridad como lo pueden ser una buena gestión de alertas y así mismo puedan dar respuesta con reacción inmediata a una contingencia ocasionada al momento de la operación.

El buen manejo de la información como lo son fuentes, análisis de datos, identificación de riesgos; genera la inteligencia de poder realizar un buen diseño aplicación de estrategias en la ejecución de los protocolos implementados y establece la continuidad operativa.

Para cualquier sistema informático es importante contar con arquitecturas de seguridad para el uso de hardware y software, lo cual se establece en el mecanismo de los dispositivos tecnológicos, desde el momento que existan sistemas de seguridad, centros de monitoreo y equipos de contingencia nos previene de un ataque ya sea en forma local o global.

Detección

Hoy día, la detección ha evolucionado, partiendo de procedimientos tradicionalistas como innovadores. Para realizar una buena custodia de la información, se propone empezar por implementar una **física** *reactiva*; esto es, poner barreras físicas que son recursos humanos operando como vigilantes, o bien, usar la tendencia de la **electrónica lógica** como lo son los CCTV, sensores, firewall que en la actualidad se encuentra en verdadero auge. Si se desea estar con líneas innovadoras, existe el desarrollo de la tecnología mediante la **seguridad inteligente**, que utiliza la biometría, análisis de imágenes, sistemas inteligentes de seguridad, etc.

Sin embargo, nace el cuestionamiento de ¿cuál es la tendencia de detección en la seguridad física? Se requiere realizar una verdadera sinergia entre la seguridad física y la seguridad lógica para realizar una convergencia y hacer sistemas con alta eficiencia que minimicen riesgos de una operación que permitan afrontar diferentes eventos. No se puede pensar en los mecanismos extremos que sean totalmente físicos y estos, a su vez, vayan a eliminar las amenazas; por tal razón, se recomienda usar en conjunto con la seguridad lógica, para poder mitigar de forma inteligente todo lo que conlleve al perjuicio de la información.

Es importante evaluar y controlar la seguridad de las instalaciones con base en la integración de una función primordial, manteniendo controlado un ambiente que ayude a disminuir siniestros y así trabajar con una sensación de seguridad, basado en el descarte de falsas hipótesis que dieran origen a diferentes incidentes.

Los grandes obstáculos que se enfrentan las organizaciones en la implementación de una buena seguridad física es: la resistencia a los cambios de nuevas estructuras, la diversidad de cultura organizacional, conflictos internos y externos, falta de comunicación, falta de liderazgo, limitaciones presupuestales, plan de acción no alineado a la convergencia, entre otros.

Por ello, con el diseño de políticas alineadas a las mejores prácticas del ISO/IEC 270002, así como el entendimiento por parte de las organizaciones de que la seguridad física-lógica es una fortaleza, dará como beneficios la reducción de costos por el uso de la tecnología, mayor capacidad de reacción inmediata, optimizará el rol preventivo y el adecuado manejo de diferentes estrategias; lo cual lleva a pensar que se generará una ventaja competitiva y hará a esta un socio estratégico.

Conclusiones

Si contamos con una buena seguridad física tanto de infraestructura, instalaciones y que además incluya la seguridad del personal (manteniendo una vigilancia y estableciendo controles) ayudará a minimizar los riesgos de las organizaciones. Lo anterior se denomina **arquitectura de seguridad de la información**, ya que durante la operación se administran las amenazas, vulnerabilidades, procesos, entre otros, que ayudan a tomar decisiones en la generación de políticas de seguridad mediante el cumplimiento de normas; asimismo nos prepara a una inteligente respuesta a un incidente, aunada a la implementación y desarrollo previos de los sistemas y habilidades de los recursos humanos para responder o recuperar la información sensible de toda organización.

Las distintas alternativas estudiadas en este trabajo se presentaron con el propósito de que no se interrumpiese el flujo de la información que pudiera llegar a afectar a cualquier organización en lo que respecta a mantener la confidencialidad, integridad y disponibilidad. Entonces, cualquier acción que se defienda de los aspectos del triángulo CID (confidencialidad, integridad y disponibilidad) [4] nos lleva a seleccionar controles adecuados que se apliquen en forma física y lógica para la defensa de la base de la información.

Referencias

[1] Huerta, A. "Seguridad en Unix y Redes". *Versión 1.2 Digital - Open Publication License v.10 o Later*. http://www.kriptopolis.org 2 de octubre de 2000.

[2] Escuela Tomás Alva Edison. www.tae.edu.mx 2007.

[3] Autoridad Nacional para la protección de la información clasificada –NS/03- Seguridad Física. Edición 2.0 http://www.cni.es/comun/recursos/descargas/NS-03_Seguridad_Fisica.pdf Diciembre 2012.

[4] Castro, S. *Arquitectura de Seguridad Informática*, Alianza de Seguridad Informática; 1a edición. Enero 24 de 2013.

Datos del Autor:

María de Jesús Antonia Ochoa Oliva

Es Ingeniera en Electrónica y Comunicaciones, cuenta con la Maestría en Teleinformática por la UANL. Es co-creadora de la carrera de la Licenciatura en Seguridad en Tecnologías de Información y de la Maestría en Ingeniería en Seguridad de la Información que se imparte en la Facultad de Ciencias Físico Matemáticas. Funge como Secretaria Administrativa del Centro de Investigación de Ciencias Físico Matemáticas y Coordinadora de la maestría antes mencionada.

Dirección del autor: Ciudad Universitaria, S/N, C.P. 66451, San Nicolás de los Garza, Nuevo León, México.

Email: maria.ochoalv@uanl.edu.mx